The Opportunities and Barriers of User Profiling in the Public Sector

Willem Pieterson, Wolfgang Ebbers, and Jan van Dijk

University of Twente, Faculty of Behavioral Sciences,
Department of Communication studies,
P.O. Box 217, 7500 AE Enschede, The Netherlands
w.j.pieterson@utwente.nl

Abstract. Like the private sector, the public sector makes more and more use of user profiling to personalize the electronic services that are being offered to citizens. User profiling offers great opportunities to make communication more effective and efficient, to infer and predict citizens' behavior and to even influence behavior. However, some drawbacks must be considered. Important differences between the private and public sector hinder the full employment of user profiling for governments and some general user profiling obstacles, such as access, trust, control and privacy have to be overcome to make fruitful use of user profiling.

1 Introduction

User profiling gives governmental organizations tremendous possibilities for their e-government strategies. Fully personalized portals, for example, provide citizens with exactly those services they need, increasing citizen satisfaction levels. It helps in making communication more effective and efficient, inferring and predicting citizens' behavior and even influencing it, in order to make citizens abide by the law. However, governments face more, different and more profound organizational obstacles than the private sector when engaging in user profiling. This paper tries to answer the question what those barriers might be and how user profiling in the public sector differs from user profiling in an e-commerce environment.

2 User Profiling

People use all kinds of ICT applications in order to support and execute the many activities that constitute their daily lives. Especially ICT applications that are aimed at providing or supporting electronic services require data on individual users to achieve their function. To give a few examples: an online store needs to have individual user data such as an address to deliver the goods that are purchased. The city administration, which is approached by an impaired citizen requesting a special parking permit near her house, must have at its disposal both data about her address and about the nature and severity of the impairment.

M.A. Wimmer et al. (Eds.): EGOV 2005, LNCS 3591, pp. 269–280, 2005.

Such data are often provided by the individual user but can be stored for re-use by the organization.

From the user's perspective, the potential benefit of a single access point is not realized when the organizations treat each contact as if it were a first-time contact. Also, from the user's perspective, single access is particularly efficient for contacts with sets of organizations or departments within organizations which in the user's opinion have a common goal or interest in the user.

Although these services might be offered by different departments or even by different organizations, the citizen will perceive them as part of one 'event' and might easily become frustrated if having to perform the entire scenario, and provide the specific data, over and over again. Re-use of data collected or provided on earlier occasions strengthens the relationship between user and organization. A good user-experience during the contact will lead to (more) satisfaction about the application used, e.g. the e-commerce or the site, and more importantly, to a (more) positive image of the organization behind the application.

The re-use of data might be done by means of user profiling. The process of using user profiles, and the underlying activities of creating, maintaining and updating user profiles, is what we will refer to as user profiling.

We define the term user profile as follows:

A user profile is a (structured) data record, containing user-related information including identifiers, characteristics, abilities, needs and interests, preferences, traits and previous behavior in contexts that are relevant to predicting and influencing future behavior [22].

Some categories of user-related information concern stable, unalterable 'properties' of the user, such as name, age and gender. Other categories relate to properties that can easily alter over time (e.g. developing new preferences or abilities) and context (e.g. having a need for information during international travel, but not during national travel). User profiling is a process that requires a long-term commitment from organizations and users. The kinds of user data collected and used imply that user profiles are regularly, if not continuously, updated with new user data.

From the organization's perspective, user profiling is a means to achieve organizational goals and/or to perform organizational activities in a more efficient and effective way. What kinds of organizational goals are to be achieved depends on the nature of the organization. For a retail organization, for example, user profiling would be a means to improve customer relationships, consequently sell more products and ultimately make more profit. For public organizations whose task is to enforce the law, user profiling is a means to increase citizens' compliance to the law. Differences in the nature of organizations determine largely how user profiling might be used in various kinds of organizations.

Both private and public organizations must build up a sound, longstanding relationship with their customers and citizens. That relationship is created and maintained by efficient and effective communication. With regards to private organizations, clients will not return if their service expectations are not met.

This will eventually lead to decreasing sales. Basically, the same also applies to governments: the Weberian principle teaches us that governments wield power over subjects, but that power is only theirs for as long as subjects allow it [29].

User profiling has additional objectives. It gives those organizations offering electronic services the possibility to gain insight into the behavior of individual users and influence them at the same time. If organizations have sufficient knowledge about their customers or citizens and are able to apply the knowledge in persuasive strategies, then they stand a better chance of organizational success. Customers will continue buying or using products and services, and citizens will be inclined more to comply with the law and only lay claim to those resources to which they are truly entitled.

3 Different Conditions for User Profiling in the Private and Public Sector

Although private and public organizations may have similar aims with user profiling, their conditions for employing user profiling are fundamentally different [24].

Public organizations are guided by *political regulation*, leading to equal rights for citizens, whereas businesses are guided by *market regulation* and differentiate between valued and less-valued customers. Businesses can afford to simply ignore less-valued customers. Public organizations have to offer their services to each citizen on an equal basis. Businesses can concentrate on the best customers that have access to technology and are motivated to use opportunities, such as those offered by user profiling. Moreover, though the private sector is restricted by consumer laws and self-regulation when applying user profiling, the public sector is much more regulated. For example, in many countries privacy regulations are much stricter for government agencies than for businesses. These two factors, (in-)equality in treating customers or citizens and the different status of regulations, will give the private sector an advantage in the innovative use of user profiling.

The government is a *referee on its own playing field* of policy, management and services. It controls its own behavior in its approach to citizens. This also means that it can enforce new laws and regulations relatively easily and quickly. This also goes for the applications of user profiling that are highly sensitive with regard to privacy and security. For example, after September 11, 2001, the American government was able to adopt the Patriot Act in only a few months. This led to highly advanced uses of data mining and user profiling of potential suspects of terrorism, thereby passing every government privacy rule and using the latest techniques developed in the corporate sector where fewer such rules exist (see for example [14]).

Unlike most businesses, the government is not a simple or straightforward organization but a *gigantic complex of organizations* on all levels and of all kinds. This means that the databases in the public sector steering each application of user profiling are more complicated (highly regulated), encompassing (every

citizen) and fragmented (a collection of basic registrations with own standards, techniques, rules, supervisions and managements) than those in the private sector. Although the integration of databases also poses problems to the private sector, the extent of these problems is incomparable to the problems envisaged in the public sector. At present, all kinds of official citizen and business registrations are being standardized and linked in networks. However, this linkage of all databases is a huge operation and will not be finished soon. The effect of this different state of affairs is that – at least for the time being – the public sector is much more preoccupied with issues concerning organization, regulation and standardization whereas the business sector is able to go ahead with innovative use of user profiling on a limited though more advanced scale. A striking example of the scale and complexity of governments is found in the United Kingdom where the National Health Service collaborates with local, regional and national authorities to develop lifelong electronic health records for 50 million patients [1]. Being very ambitious, this is an enormous operation that takes the next 10 years to be fully operational and involves dozens of organizations and thousands of people in order to be a success.

In comparison with the public sector, the private sector made considerable progress with the tailoring of products and services in the course of the 20th century. The drive to reach individual consumers was simply much stronger than the drive for governments to communicate with individual citizens. Customers can choose where to buy products and services and businesses need to sell their products and shall therefore always compete with their competitors for the favor of the customer. Therefore, market research, bookkeeping and records of buying and selling have dominated corporate activities for the past 150 years. The corporate sector has invented technologies of group segmentation, direct marketing, market research, individual customer relationship marketing etc. In contrast, the *government lacks the experience* with those innovations but has on the other hand accumulated considerable experience with compiling and maintaining enormous registrations of citizens, real estates, enterprises etc. It has therefore become an expert in using personal information on an enormous scale, for example in printed and electronic forms.

Unlike most businesses, public organizations have a *monopolistic proposition*. In comparison to commercial clients, citizens have no options to change to another service provider. So on first sight, there seems to be no threat to the rationale of the existence of governmental agencies as there is no market place competition (see also above). For that reason, there seems to be no urgent need to upgrade e-government services to the level of personalized e-services in order to keep customer satisfaction at a high level, which has been a very important driver for businesses in the personalization movement. But that doesn't mean that public servants won't have to bother and won't sense any pressure at all to improve their services. Because as soon as performances drop beneath acceptable levels chances are that the public starts to complain. When this situation prolongs radical top-down interventions like outsourcing are on the verge. For

instance, this year the Dutch Tax Office decided to outsource parts of its call center activities once number of complaints about the service grew.

In the course of the 1990s, public opinion, political pressure and competition (e.g. losing services through privatization) forced government departments to become more user-oriented towards their citizens or clients, to integrate their fragmented service counters, to save on the administrative costs imposed on citizens and corporations and to supply all kinds of user-driven electronic applications. Suddenly, government departments adopted all kinds of customization technologies from the commercial sectors in order to become more service-oriented and user-centered (see for example [3]). In the first decade of the 21st century, however, attention and priorities have again shifted to law enforcement and security issues (due to e.g. September 11, 2001). Nowadays, both objectives, i.e. user-driven electronic services and screening or surveillance applications, may fuel the need for government user profiling.

4 Organizational Obstacles to User Profiling

Offering personalized services might imply that the user is given an important role in the way the business process is designed and implemented. It is even possible to give customers access to all kinds of back-office systems, for example to place an order directly in the organization's back-office, as it is the case with electronic banking and many internet stockbrokers and internet stores. Or to enable the users to control and maintain the user profile themselves, instead of the organization [17]. Examples of applications that enable user control are for instance applications such as MSN and ICQ.

This means that an organization's production and logistical processes must be able to cope with it. If that is not the case, the information systems (see below) and the processes will have to be redesigned. In general, redesign processes and reorganizations are complicated and they cost (at least) time and money (see for example [22], [20]). In one way or another, these costs will have to be considered in the investment proposal.

Another organizational obstacle in user profiling is the question who is responsible for what, especially when more than one organization make use of the profile. Not only do control issues have to be arranged with citizens (as will be discussed further on), but also within the government when organizations are collaborating, who will keep the user profile up-to-date? Who is entitled to make changes? In these circumstances it is necessary that there are clear procedures and processes to indicate which department and which officials (and how) have access and are responsible for an electronic file. The painstaking introduction of the Electronic Patient Record (EPR) in the Netherlands is proof that it is not always easy to agree on standards and processes [4]. Discussions on the use of a single personal identification number, a medication record and billings systems held up the introduction of the EPR for years. A solution might be to create an organization, or spot within the government, where control is being exercised. Because this means a change in the lines of responsibility for and being account-

able to, some shift in organizational tasks and responsibilities will have to take place. The resulting shifts in power constitute a delaying factor [25].

Legal obstacles also face governments. As discussed previously in this paper, legal conditions for public organizations engaging in user profiling are governed by political regulation, which is different from the market regulation guiding the private sector. Privacy infringement issues and the risk for citizen exclusion make it for instance difficult for governments to adopt user profiling strategies from the commercial sector. Another obstacle is relevant when public organizations start to collaborate and start offering joint services. In public administration it is important that collaboration is legally recorded, if only for the protection of the public's interests. It is important that the division of powers, the decision-making structure and the scope for influencing are clear. And there must also be supervision, democratic control and publicity. Collaboration on the basis of mutual agreement can occur between municipalities, provinces and district water boards or a combination of these three. Also national governments can participate. Such an agreement has to comply with quite a number of regulations (see for example [26], for a discussion about collaboration between Dutch municipalities).

5 User Obstacles to User Profiling

In order to implement user profiling, organizations have to overcome a number of hurdles on the user side of user profiling. First, users need to have access to ICT, in order to be able to use their user profile. Second, the user has to accept the use of user profiling. This acceptance is determined by trust, control and privacy issues.

5.1 Access

Access to ICT is a basic requirement to engage in user profiling. Access is not limited to the possession of ICT, access is also about the motivation and the skills to use ICT [23]. In general three groups of users can be distinguished, according to the intensity of usage and acceptance of applications that take advantage of user profiles. Probably, these groups do not differ significantly from those that use and accept ICT and new media in general. There are no reasons to suppose that the divide in use and acceptance of user profiles will differ from the existing 'generic' digital divide.

The first group is the *information elite*. The information elite consists of active information seekers and communicators, strongly motivated to use the digital media. They have complete and multi-channel physical access, and they are experienced users who possess the required operational, information and strategic skills. They might be the ones most interested in user profile applications, but they are also the most critical users. Several niche markets of user profiling applications can be explored for the information elite.

The second group is the *electronic middle* class. About 55 percent (the majority) of the population in developed high-tech societies has access to the digital

media, usually only one or two channels (at home and at work). They use the digital media only for a few purposes, first of all for entertainment and secondly, for simple applications of information, communication and transaction. Only very basic, highly accessible, user friendly and trustworthy user profiling applications will attract their attention, which are consequently the only applications that are appropriate for a mass market.

The third and final group consists of the *digital illiterates*. The unconnected and the non-users form about one third (30%) of the population in developed high-tech societies. With no access to computers and the Internet, they only use digital media such as televisions, telephones and audio-visual equipment. Within this group, the elderly (over 65), unemployed women, people with little education, people with a low income, disabled people and migrants or members of ethnic minorities are over-represented. A large proportion of these groups lacks the motivation, the resources and the skills to use computers, the Internet and complicated other digital media. All the conditions for effective user profiling applications are simply absent among this part of the population. This is an important issue for government services in particular, as they are supposed to reach the entire population. Solving this problem requires additional effort in providing basic public access sites (of computers and the Internet) with service staff and/or similar applications of user profiling on the basis of old media (print media, telephony and face-to-face service).

5.2 Acceptance

Acceptance is a complex issue that transpires through the whole user profiling framework. Users and organizations have to accept each other, ICT has to be accepted and finally the user profile has to be accepted. Acceptance is a continuous process that does not stop when the decision is made to adopt user profiling. People are unstable in their preferences and behavior, so it might well be possible that an individual accepts the use of his user-related information at a certain point in time, for example because it offers direct benefits, but is not willing to accept it at another time. Organizations should therefore pay attention to user acceptance throughout the creation, implementation and use of user profiles. A few factors are especially relevant for acceptance, these factors are trust, control and privacy.

Perhaps the most essential additional factor determining acceptance is *trust*. Trust is a critical factor for the adoption and acceptance of new technologies and is generally accepted as a prerequisite for good personalization practice [6]. Users are not likely to reveal confidential information about themselves to an untrustworthy party, and they may be suspicious of data harvesting practices if they feel the information may be misused in some way. Research [16] demonstrated that lack of trust was the major reason for people not to adopt online shopping. Warkentin, Gefen, Pavlou, and Rose [28] studied the role of trust in the adoption of e-services. They found that trust in the organization using the technology and trust in governmental policies are important determinants for the adoption. They state that trust is a crucial enabler affecting purchase inten-

tions, inquiry intentions and the intention to share personal information. The latter intention, of course, is especially relevant in user profiling. Dahlberg, Mallat & Öörni [11] interviewed participants in a focus group about the factors that determined their decision to adopt mobile payment services. Trust proved to be an important factor for the acceptance of these services. Gefen, Karahanna and Straub [15] have studied trust in online shopping. They state that trust influences the intention to buy online. Finally, Brigss et al. [6] point to the fact that trust and personalization have a reciprocal relationship. Trust is not only a prerequisite for good personalization, good personalization also generates trust.

The second acceptance factor is control. A study by Roy Morgan Research [19] shows that 59% of the 1524 Australian respondents in a survey state that their trust in the Internet increases when they feel they have control over their personal information. The study also showed that:

- 91% of the respondents want to be asked for explicit permission before companies use their information for marketing purposes;
- 89% of the respondents want to know which persons and which organizations have access to their personal information;
- 92% of the respondents want to know how their personal information is used.
- User control obviously is a critical condition for user acceptance of profiling and personalization. However, the study cited does not answer the question whether the users themselves should host the user profile themselves, nor whether trusted third parties can resolve the users' anxiety about control issues.

Alpert et al. [2] studied user attitudes regarding the personalization of content in e-commerce websites. In their study, the users expressed their strong desire to have full and explicit control of personal data and interaction. They want to be able to view and edit (update and maintain) their personal information at any time.

Byford [7] perceives personal information as a property or asset of the individual ('Byford's property view'). The user is the owner of his or her personal information. In Byford's property view, individuals see privacy as the extent to which they control their own information in all types of Internet exchanges. The property aspect of the exchange manifests itself in the users' willingness to trade personal information for valued services such as free e-mail or special discounts from merchants.

A user profiling system that is not supported by a good system for user control of personal information is bound to lead to acceptance problems. However, building a user interface that allows users to control the information in their profiles is a complicated problem, especially if the interface provides controls that go beyond a very course level of granularity [8]. Although users have indicated they want to be in control of their personal data, very little users make use of the possibilities that websites offer to control personal information. A number of ecommerce web sites give users access to their profiles; however, it is unclear that many users are aware of this [8]. Reports of operators of personalization

systems have indicated that users rarely take actions to proactively customize their online information [18].

The third factor determining acceptance is privacy. Wang, Lee and Wang [27] distinguish four types of privacy threats:

- improper acquisition of information (e.g. uninvited tracking of the users' web usage);
- improper use of information (e.g. distribution of data to third parties);
- privacy invasion (e.g. spamming a mailbox with uninvited direct mailings);
- improper storage and control of personal information (e.g. no opting-out, no means to remove incorrect or unwanted information)

It is still unclear which privacy threats and concerns are (most) influential for acceptance of user profiling. But it is clear that privacy is important for the users' acceptance of internet, and hence for acceptance of user profiling. An overview of studies regarding privacy and personalization on the Internet shows that users have significant concerns over the use of personal information for personalization purposes on the Internet [21]. CyberDialogue [10] found that 82% of all Internet users say that a website's privacy policy is a critical factor in their decision to purchase online. Even more salient is that 84% of the respondents have refused to provide information at a website because they were not sure how that information would be used. The fact that there is a concern, however, does not necessarily imply that users don't provide any information. The lack of trust in privacy policies moved a large majority of users to give false or fictitious information over the Internet, and thus protect their privacy [9], [13]. Examples of this development include 'Anonymous Web surfing' and the use of pseudonyms. According to research conducted by the Winterberry Group, this development is increasingly becoming a problem for the collection of user related information [12]. It also makes it apparent that many users are reluctant about user profiling.

Users might be willing to sacrifice some privacy and trade personal information, in exchange for recognizable rewards, such as information that suits their needs or preferences better. But even in the case they are willing to give up their parts of their privacy, they have to be reassured that their personal information is not used in ways they do not approve. Mander, Patel and Robinson [18] suggest two solutions to address privacy concerns: make use of encryption of passwords and sensitive data to guard information (possibly external) audit and evaluation procedures for data security and privacy issues. Bonett [5] states that organizations should declare a privacy statement (or disclosure statement) on their site, which describes the kinds of information gathered and the policies for using and sharing personal information.

6 Concluding Remarks

As this paper shows, user profiling has opportunities for governments in their e-government strategies. However, although the possible benefits are numerous,

there are some specific hurdles to be taken such as legal, and governance obstacles, which hinder the development of user profiling.

For governments it does not suffice to fully adopt user profiling strategies from the private sector. The conditions for employing user profiling simply differ too much from the private sector. In contrast to the private sector, for the public sector widespread acceptance of user profiling and personalized e-government services is of the utmost importance, since public organizations have to offer their services to each citizen on an equal basis. This creates problems for citizens who lack sufficient computer skills to create, maintain, use or control a user profile, let alone to those who simply don't have any internet access. For that reason, in the public sector users should play a much more important role in developing and implementing personalized e-services then in the private sector.

However, when doing so governments should be aware of a diffusion paradox. For a successful diffusion governments should start with those who are able to handle complicated applications: the information elite. However, the information elite is known for its critical attitude towards user profiling and leaving behind personal information on the internet. So there may be some initial resistance when members of the information elite are invited.

Another though nut to crack is that once diffusion has started the information elite has an advantage over other, less computer skilled citizens. To balance this unequal situation the latter have to be supported in order to catch up with the information elite. In conclusion, when investing in personalized e-services governments also have to consider educational programs in order to make life easier to all members of society, and not only to the happy few.

7 Future Research

This paper argues that, besides differences between the public and private sector, both organizational obstacles and user obstacles may possibly hinder the use of user profiling. The organizational obstacles mentioned here are organizational and legal obstacles. The user obstacles discussed are trust, the control of the user profile and privacy concerns. Future research addressing these obstacles would be useful for further e-government developments. For governments it would be wise to develop own, public sector specific, strategies. This would increase the changes for successful user profiling and helps to avoid the obstacles described in this paper.

The described obstacles, as well as the differences between the public and private sector all have consequences for the development of user profiling for governments. Many of the obstacles are closely related, for example, giving user direct access to back offices to change their profile is technically challenging, thus posing a technical obstacle, and expensive to solve, posing a financial obstacle. When privacy concerns are not solved, it is unlikely that users will trust user profiling.

The strong relationship between the various concepts has its consequence for user profiling. Nowadays we see that governments as well as businesses are trying

to take away some of the obstacles, for example by using a privacy statement on their websites to solve privacy concerns. Other organizations let users control their own data. The intertwinement of the various concepts however asks for more than taking away the separate hurdles, what we need is a more integrated view of user profiling, its obstacles and the solutions to those obstacles. This integrated perspective should be a main topic of research in the next years.

References

1. Accenture: Leadership in Customer Service: New Expectations, New Experiences. Accenture, (2005)
2. Alpert, S.R., Karat, J., Karat, C.-M., Brodie, C., Vergo, J.G.: User attitudes regaring a User-Adaptive eCommerce Web Site. User Modelling and User-Adapted Interaction, 13(4) (2003) 373-396
3. Bekkers, V.J.J.M.: E-government: meer dan e-commerce voor overheden. Tijdschrift management & informatie, 8(2) (2000) 11-20
4. Berg, M.: Kaf en Koren van kennismanagement: Over informatietechnologie, de kwaliteit van zorg n het werk van professionals (inaugurele rede). Erasmus Universiteit, Rotterdam (2001)
5. Bonett, M.: Personalization of Web Services: opportunites and Challanges. Ariadne Magazine (28) (2004)
6. Briggs, P., Simpson, B., De Angeli, A.: Personalisation and Trust: A reciprocal Relationship? In: Karat, C.-M., Blom, J.O. and Karat, J. (eds.): Designing Personalized user experiences in eCommerce. (2004)
7. Byford, K.S.: Privacy in Cyberspace: constructing a model of privacy for the electronic communications environment. Rutgers Computer and Technology Law Journal (24) (1998) 1-74
8. Cranor, L.F.: I Didn't buy it for myself: Privacy and ecommerce personalization. In: Karat, C.-M., Blom, J.O. and Karat, J. (eds.): Designing Personalized user experiences in eCommerce. Kluwer Academic Publishers, Dordrecht (2004)
9. Culnan, M.J., Milne, G.R.: The Culnan-Milne survey on consumers & online privacy notices: Summary of Responses. In: Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices. Washington DC, (2001)
10. CyberDialogue: Online consumer personalization survey. The personalization consortium, Wakefield (2001)
11. Dahlberg, T., Maalt, N., Öörni, A.: Trust enhanced technology acceptance model – consumer acceptance of mobile payment solutions. Helsinki school of economics, Helsinki (2004)
12. Direct Marketing: Anonymous Web Browsing Threatens Profiling Practices of E-marketers. (2001)
13. Fox, S., Raine, L., Horrigan, J., Lenhart, J., Spooner, T., Carter, C.: Trust & Privacy Online: Why Americans want to rewrite the rules. The Pew Internet & American Life Project, Washington DC (2000)
14. GAO: Data Mining. Federal Efforts cover a wide range of uses. United States General Accounting Office, (2004)
15. Gefen, D., Karahanna, E., Straub, D.W.: Trust and TAM in Online Shopping: An Integrated model. MIS Quarterly, 27(1) (2003) 51-90
16. Hoffman, D.L., Novak, T.P., Peralta, M.: Building consumer trust online. Communications of the ACM, 42(4) (1999) 80-85

17. James, H.: Customer-Centric E-business. Business Communications Review, 30(8) (2000)
18. Manber, U., Patel, A., Robinson, J.: Experience with personalization on Yahoo! Communications of the ACM, 43(8) (2000) 35-39
19. Roy Morgan Research: Privacy and the community. (2001)
20. Silverman, M.J., Weinstein, A.J.: INDOPCO and the fax treatment of reorganization costs. Tax executive, 49(1) (1997) 31
21. 21. Teltzrow, M., Kobsa, A.: Impacts of User Privacy preferences on personalized systems: acomparative study. In: Karat, C.-M., Blom, J.O. and Karat, J. (eds.): Designing personalized user experiences for eCommerce. Kluwer Academic Publishers, Dordrecht (2004)
22. van der Geest, T.M., van Dijk, J.A.G.M., Pieterson, W.J. (eds.): Alter Ego: State of the art on user profiling. An overview of the most relevant organisational and behavioural aspects regarding User Profiling. Telematica Instituut, Enschede (2005)
23. van Dijk, J.A.G.M.: The Deepening Divide, inequility in the information society. London: Thousand Oaks (2005)
24. van Dijk, J.A.G.M.: e-Government. In: Bouwman, H., van Dijk, J.A.G.M., van den Hooff, B. and van de Wijngaert, L. (eds.): ICT in Organisaties. Boom, Amsterdam (2002)
25. van Venrooy, A.: Nieuwe vormen van interorganisationele publieke dienstverlening. Eburon, Delft (2002)
26. Vereniging van Nederlandse Gemeenten (VNG): Intergemeentelijke samenwerking en ICT: De grenzen verkennnen. VNG, Den Haag (2003)
27. Wang, H., Lee, M.K.O., Wang, C.: Consumer Privacy concerns about Internet marketing. Communications of the ACM, 41(3) (1998) 63-70
28. Warkentin, M., Gefen, D., Pavlou, P.A., Rose, G.M.: Encouraging citizen adoption of e-Government by building trust. Electronic Markets, 12(3) (2002) 157-162
29. Weber, M.: Gezag en bureaucratie: Geredigeerd en ingeleid door prof. dr. A. van Braam. Universitaire Pers Rotterdan, Rotterdam (1970)